



Calhoun: The NPS Institutional Archive

News Center

News Articles Collection

2008-06

CHDS Sponsors Critical Infrastructure Protection Workshop

Center for Homeland Defense and Security

Naval Postgraduate School, Monterey, California

<http://hdl.handle.net/10945/51329>



Calhoun is a project of the Dudley Knox Library at NPS, furthering the precepts and goals of open government and government transparency. All information contained herein has been approved for release by the NPS Public Affairs Officer.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943

<http://www.nps.edu/library>

CHDS Sponsors Critical Infrastructure Protection Workshop



The NPS Center for Homeland Defense and Security in partnership with the U.S. Department of Homeland Security recently hosted its first Critical Infrastructure Protection Workshop. The workshop brought together practitioners and academics from around the world to discuss risk assessment metrics, methods, and tools.

One of the fundamental missions of the DHS, in partnership with state and local governments and tribal authorities is to protect the critical infrastructure and key resources of the United States against terrorist attacks. The overview of the National Infrastructure Protection Plan states (<http://www.dhs.gov/nipp>)

“The National Infrastructure Protection Plan (NIPP) and supporting Sector-Specific Plans (SSPs) provide a coordinated approach to critical infrastructure and key resources (CI/KR) protection roles and responsibilities for federal, state, local, tribal, and private sector security partners. The NIPP sets national priorities, goals, and requirements for effective distribution of funding and resources which will help ensure that our government, economy, and public services continue in the event of a terrorist attack or other disaster.



The plan is based on the following:

- Strong public-private partnerships which will foster relationships and facilitate coordination within and across CI/KR sectors.
- Robust multi-directional information sharing which will enhance the ability to assess risks, make prudent security investments, and take protective action.
- Risk management framework establishing processes for combining consequence, vulnerability, and threat information to produce a comprehensive, systematic, and rational assessment of national or sector risk.”

“However, five years after the creation of the requirement, a robust risk management framework has yet to be created,” said CHDS professor Tom Mackin. “More troublesome is that, among the various constituents, there is no universally accepted definition of risk and no standards for assessing vulnerability or consequences. This has led to a patchwork of conflicting and confusing methods that make it impossible to allocate resources efficiently to best protect the nation.”

The goal of the workshop was to reach a consensus on the underlying fundamentals of risk assessment to substantiate any tools or methods currently in use. A team of experts were assembled to form scholarly papers and oral presentations on risk, consequence, and vulnerability. A significant part of the presentations included an implementation of methodology in the form of a procedure, software application, or case study that a practitioner may directly apply to the problem of risk assessment of critical infrastructure. “The workshop created a forum to discuss best practices, share methods, and direct better choices,” said Mackin.

“This is a ground-breaking event because it is the first time academics and practitioners have gotten together to discuss risk assessment for critical infrastructure protection,” said CHDS Executive Director, Ted Lewis.

All workshop proceedings, papers and presentations are available for review.

